Office of Transportation Vetting and Credentialing

Transportation Worker Identification Credential (TWIC)

Transportation Security Administration

TWIC Program Brief: Outline

- TWIC Program Overview
- Governing Legislation
- Program Phases
  - Phase I: Planning
  - Phase II: Technology Evaluation
  - Phase III: Prototype
- Current Status - Phase III: Prototype
  - Prototype Timeline
  - Prototype Participants
  - Prototype System Components
    - Identity Management System
    - Enrollment
    - Vetting
    - Card Production
- TWIC: A Standards-Based Program
- Homeland Security Presidential Directives 11 and 12
- TWIC Program Definitions

TWIC Program

Vision

A high-assurance identity credential that is trusted and used across all transportation modes for unescorted physical access to secure areas and logical (cyber) access to systems.

Goals

- Improve security
- Enhance commerce
- Protect personal privacy

TWIC Program (continued)

What is a TWIC?

TWIC is an acronym for *Transportation Worker** Identification Credential. The Transportation Security Administration (TSA) is currently testing a system-wide common credential to be used across all transportation modes, for all personnel requiring unescorted physical and/or logical (i.e. computer) access to secure areas of the transportation system. The TWIC will positively tie the person - to the credential - to the threat assessment.

What are the security problems currently faced by the various modes of our transportation system and supply chain that TWIC aims to solve?**

- Inability to positively identify individuals entering secure areas of the transportation system;
- Inability to assess the threat posed to the transportation system by individuals due to a lack of background information, or the lack of uniformly determined background information; and
- Inability to protect current credentials against fraud.

* *Italicized* words are defined in the TWIC Program Definitions section of this brief
** Responses taken from the TWIC Mission Need Statement (MNS), April 2004, page 1

TWIC Priorities

Strong focus on identity assertion

- Establish and maintain the integrity of the chain of trust for identity management by binding the cardholder-credential-biometric-threat assessment-valid user

Drive excellence in use of biometrics for physical access solutions

- American National Standards Institute (ANSI) standard photograph/fingerprint minutiae/fingerprint pattern/Iris

TWIC Program Benefits

Improves Security

- Reduces risk of fraudulent or altered credentials;
- Employs *biometrics** for secure, positive match of individual to authorized facility access points;
- Supports ability to interface and communicate with other agencies; and
- Provides timely system-wide revocation.

Enhances Commerce

- Eliminates need for multiple credentials and background checks;
- Leverages current security investment and existing systems;
- Maintains process speed and efficiency;
- Expands e-government potential;and
- Enables public-private partnership.

Protects Personal Privacy

- Collects minimal personal information;
- Uses a secure record control system and network;
- Employs advanced information technology to protect personal information; and
- Incorporates system-wide encryption.

* *Italicized* words are defined in the TWIC Program Definitions section of this brief

Governing Legislation

Maritime Transportation Security Act of 2002 (MTSA)

Requires the issuance of biometric transportation security cards and the completion of background checks for entry to any secure area of a vessel or *facility**.

Aviation and Transportation Security Act of 2001 (ATSA)

Directs strengthened access control points in airport secured areas and requires TSA to consider the use of biometric or similar technologies, that identify individuals employed at airports.

* *Italicized* words are defined in the TWIC Program Definitions section of this brief

Program Phases

☑ Planning

‘As-Is’ Analysis

‘To-Be’ Analysis

Requirements Baseline

Technology Evaluation Plan

Site Survey

Methodology & Performance Metrics

Technology Demo

☑ Technology Evaluation

East & West Coasts

Evaluate Range of Potential Technologies for Core Business Process and Requirements

Multiple Facilities

Five Technologies:
Integrated Circuit Chip
Optical Memory Stripe
Magnetic Stripe
Linear Bar Code
2-D Bar Code

Cost-Benefit & Life-Cycle Cost Analysis

Prototype*

East, West, and FL

Evaluate Access Technologies for Full Range of Business Processes, Policies and Requirements

Biometrics

Additional Facility Locations

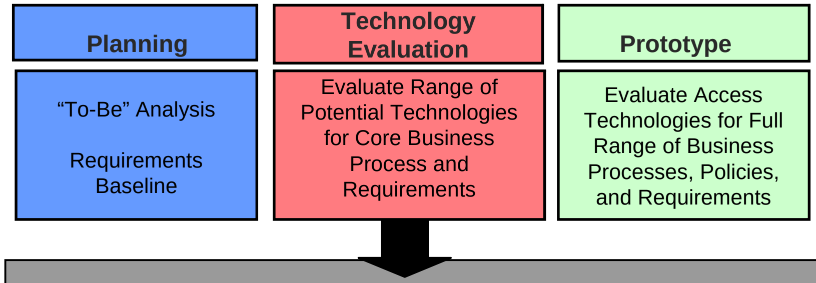
TWIC Technology Prototype (Multi-Tech Card)

Policy & Processes Include:
Trusted Agent
Claimed ID
Migration Across Region

☑ **Completed**

*Currently in Prototype Phase

Technology Evaluation Accomplishments



Planning

"To-Be" Analysis

Requirements Baseline

Technology Evaluation

Evaluate Range of Potential Technologies for Core Business Process and Requirements

Prototype

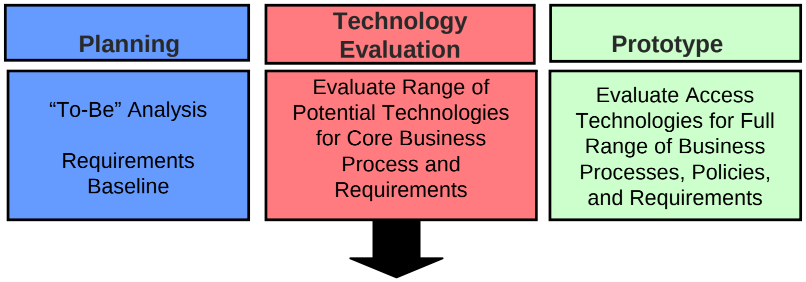
Evaluate Access Technologies for Full Range of Business Processes, Policies, and Requirements

- **Tested five card-based technologies at 12 transportation facilities in two regions:**
  - *Integrated Circuit Chip**
  - Optical Memory Stripe
  - 2-D Barcode
  - Linear Bar Code
  - Magnetic Stripe
- **Issued cards to a broad range of transportation workers:**
  - Union workers (ILWU, AFL-CIO, etc.)
  - Non-union workers, managers, owners
  - Airline mechanics
  - Independent truck drivers
  - Security guards
  - Railroad employees
  - Crane operators
  - Pipeline workers
  - Tug boat crews
- **Evaluated each technology in a variety of physical and logical access transactions:**
  - Vehicle gates
  - Truck multi-lanes
  - Unattended gates
  - Staffed guard stations
  - Unattended building entrances
  - High volume pedestrian turnstile
  - IT system sign-on
  - Internal building doors
  - Parking garage exit points
- **Evaluated central card production feasibility:**

  Produced the final increment of cards for the West Coast region at the U.S. Customs and Immigration Service facility in Corbin, KY
- **Operated enrollment centers, local issuance, help desk, and card management systems.**

**Italicized* words are defined in the TWIC Program Definitions section of this brief

Prototype Goals



Planning	Technology Evaluation	Prototype
"To-Be" Analysis Requirements Baseline	Evaluate Range of Potential Technologies for Core Business Process and Requirements	Evaluate Access Technologies for Full Range of Business Processes, Policies, and Requirements

The three primary goals of the TWIC Prototype Phase are as follows:

1) Assess performance of the TWIC *identity management** architecture and business processes to determine the best strategy for potential implementation;**

2) Assess performance of TWIC as an access control tool; and

3) Evaluate readiness of TWIC system for implementation** phase.

These goals are explained in greater detail in the following slides.

Transportation
Security
Administration

* *Italicized* words are defined in the TWIC Program Definitions section of this brief

** Upon completion of the Prototype Phase and review of the Prototype Final Report and program recommendations, the decision for full implementation will be made.

Prototype Goals

1) Assess performance of the TWIC identity management architecture and business processes to determine the best strategy for potential implementation. This includes:

   - Evaluating sponsorship process;
   - Verifying *claimed identity*;*
   - Capturing biographic (e.g. name) and biometric information;
   - Conducting terrorist threat assessments;
   - Producing batches of high quality, tamper resistant cards;
   - Confirming operation of IT infrastructure;
   - Conducting testing of contactless card;
   - Evaluating options for issuance modes and locations; and
   - Evaluating privacy and policy issues.

* *Italicized* words are defined in the TWIC Program Definitions section of this brief

Prototype Goals

2) Assess performance of TWIC as an access control tool. This includes:
   - Evaluating *contactless smart card** technology with biometrics as an access control tool;
   - Confirming operation of facility / TWIC interfaces;
   - Confirming effectiveness of *revocation** capability; and
   - Evaluating the TWIC as a tool for local authorities to grant access.

3) Evaluate readiness of TWIC system for Implementation** Phase. This includes:
   - Developing a comprehensive Prototype Final Report with a detailed cost benefit analysis; and
   - Evaluating the options of federal role vs. state/private industry role.

Transportation
Security
Administration

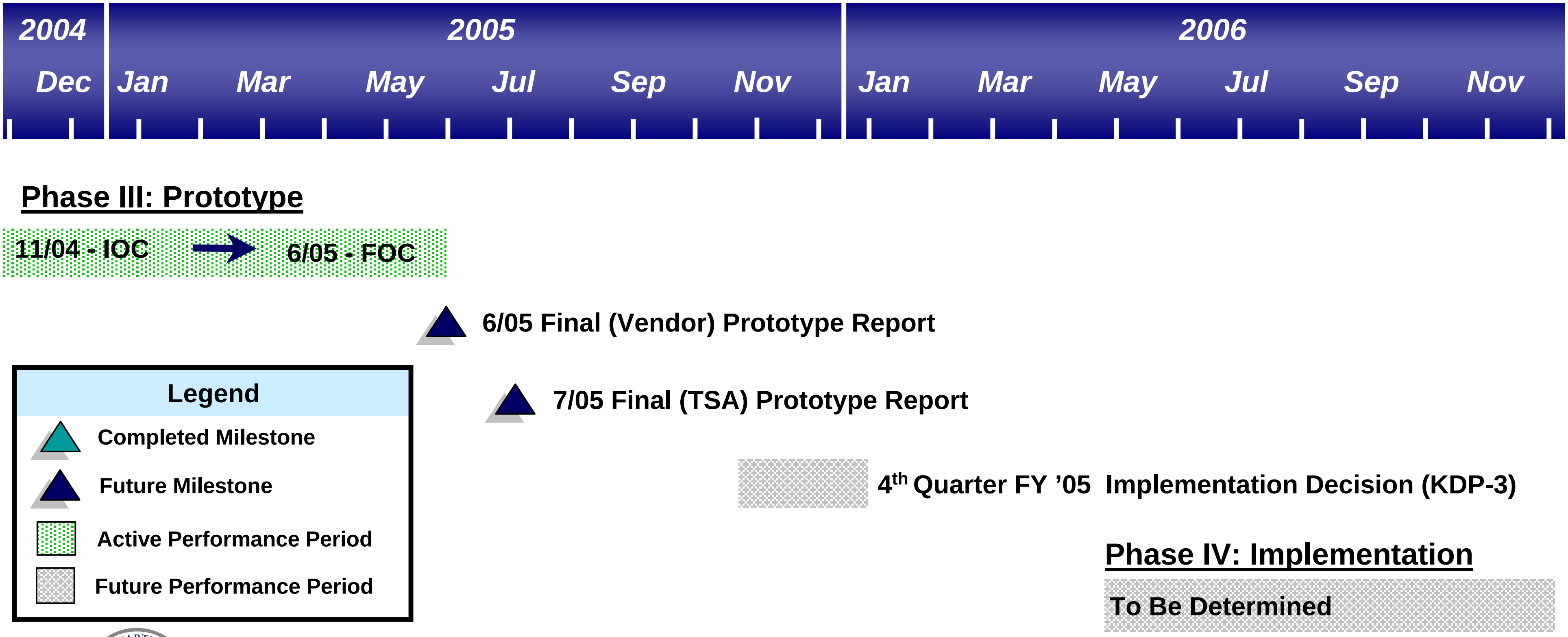
* *Italicized* words are defined in the TWIC Program Definitions section of this brief

** Upon completion of the Prototype Phase and review of the Prototype Final Report and program recommendations, the decision for full implementation will be made.

Prototype Timeline

Where is TSA in the process of issuing TWICs to transportation workers?

Prototype is the third phase of the TWIC Program and follows the successful completion of the planning and technology evaluation phases in 2003. The goal of Prototype is to assess the performance of the TWIC identity management business processes.



Phase III: Prototype

11/04 - IOC → 6/05 - FOC

▲ 6/05 Final (Vendor) Prototype Report

▲ 7/05 Final (TSA) Prototype Report

▨ 4th Quarter FY ’05 Implementation Decision (KDP-3)

Phase IV: Implementation

To Be Determined

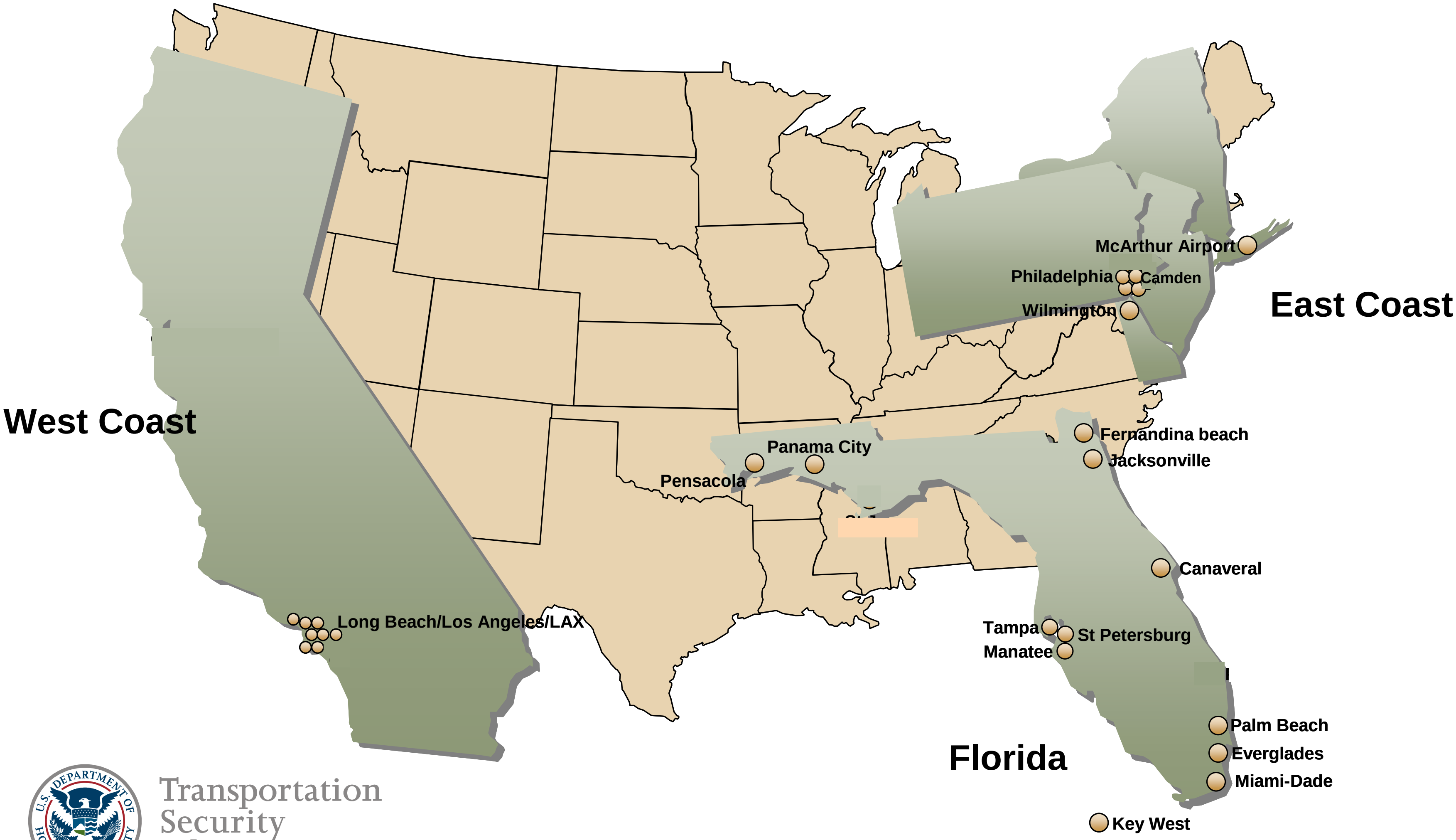
Legend

- ▲ Completed Milestone
- ▲ Future Milestone
- 🟩 Active Performance Period
- ▨ Future Performance Period

Transportation Security Administration

Prototype Participants

Participants include transportation workers from maritime, rail, aviation and ground transportation facilities. Each circle represents a participating transportation facility.

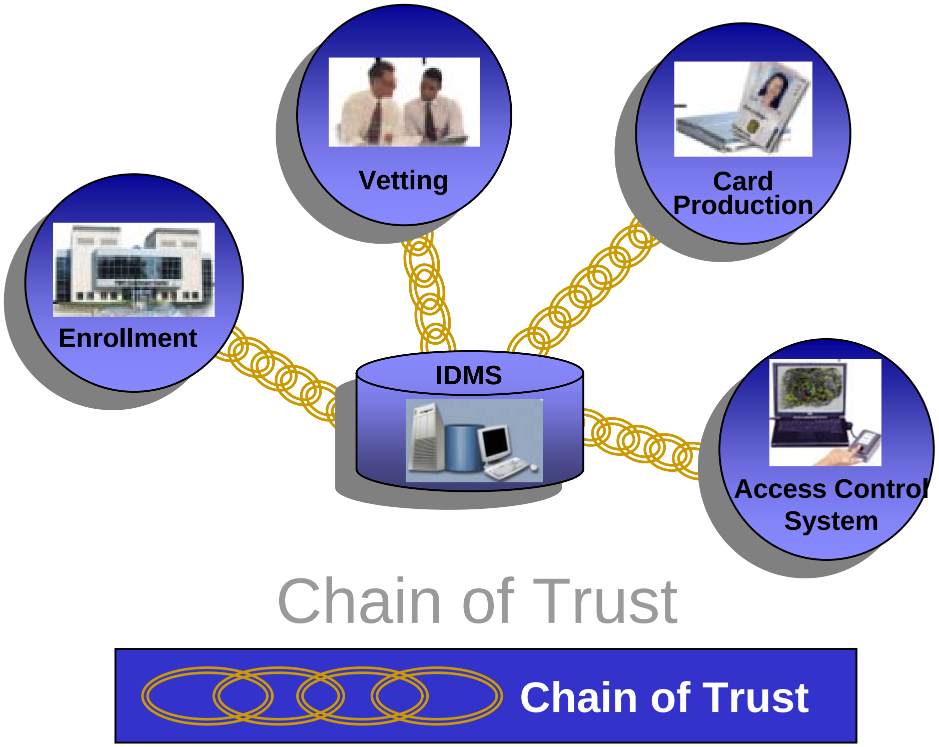


Transportation
Security
Administration

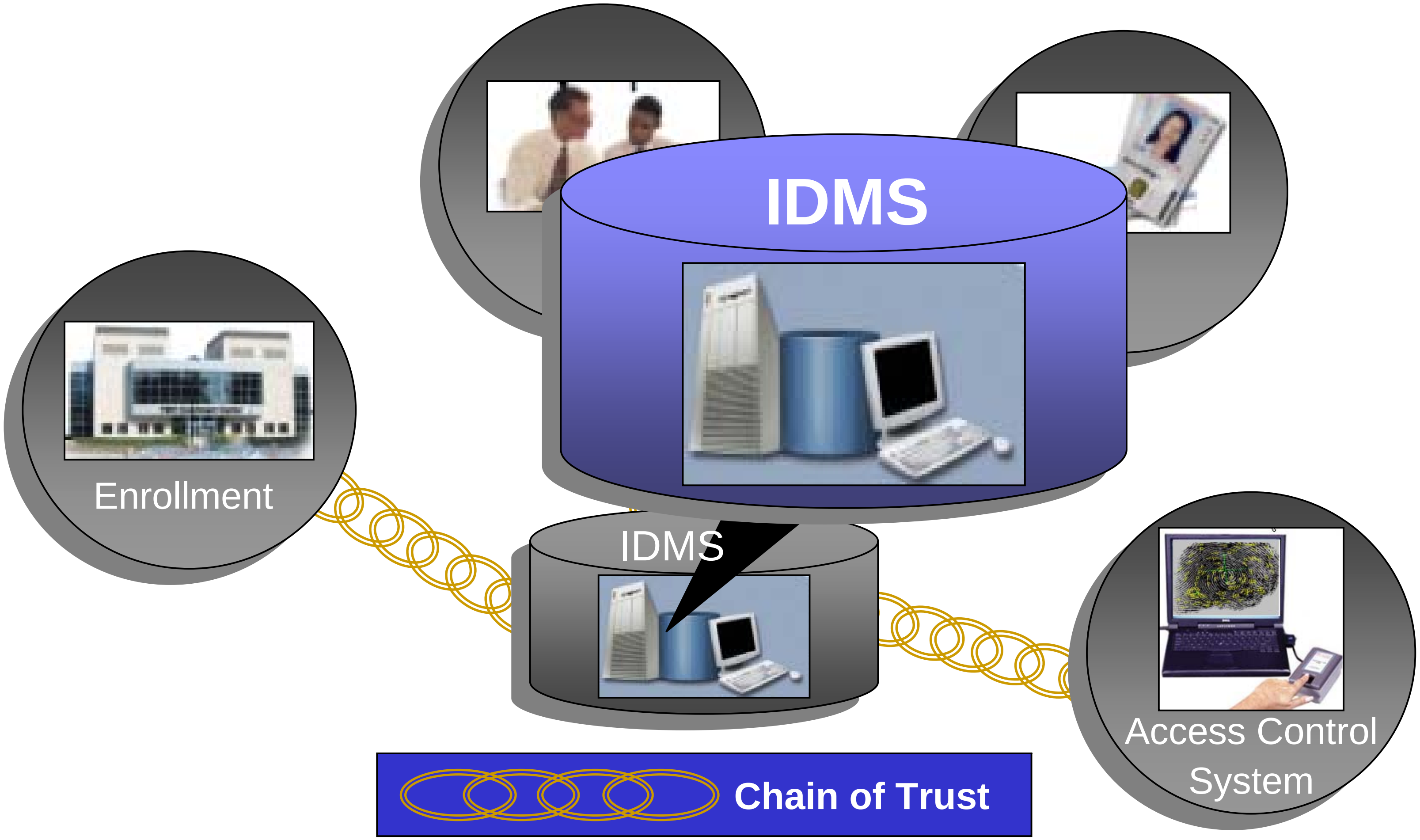
Chain of Trust: Prototype Components

The chain of trust is a concept used in the TWIC Program that describes the nature of the relationship between the prototype system components. “Chain of trust” refers to the Program features that ensure personal privacy and security through people, technology, and process to obtain, transfer and manage personal information. These include:

- The use of “Trusted Agents,” personnel who are trained and certified to handle personal information;
- Advanced information technology that includes such tools as encryption and biometrics to ensure the security and integrity of personal information; and
- Strict standards for performance and business processes. These include system audits to evaluate and improve security.



Prototype System Components



IDMS

Enrollment

IDMS

Access Control System

Chain of Trust

Identity Management System

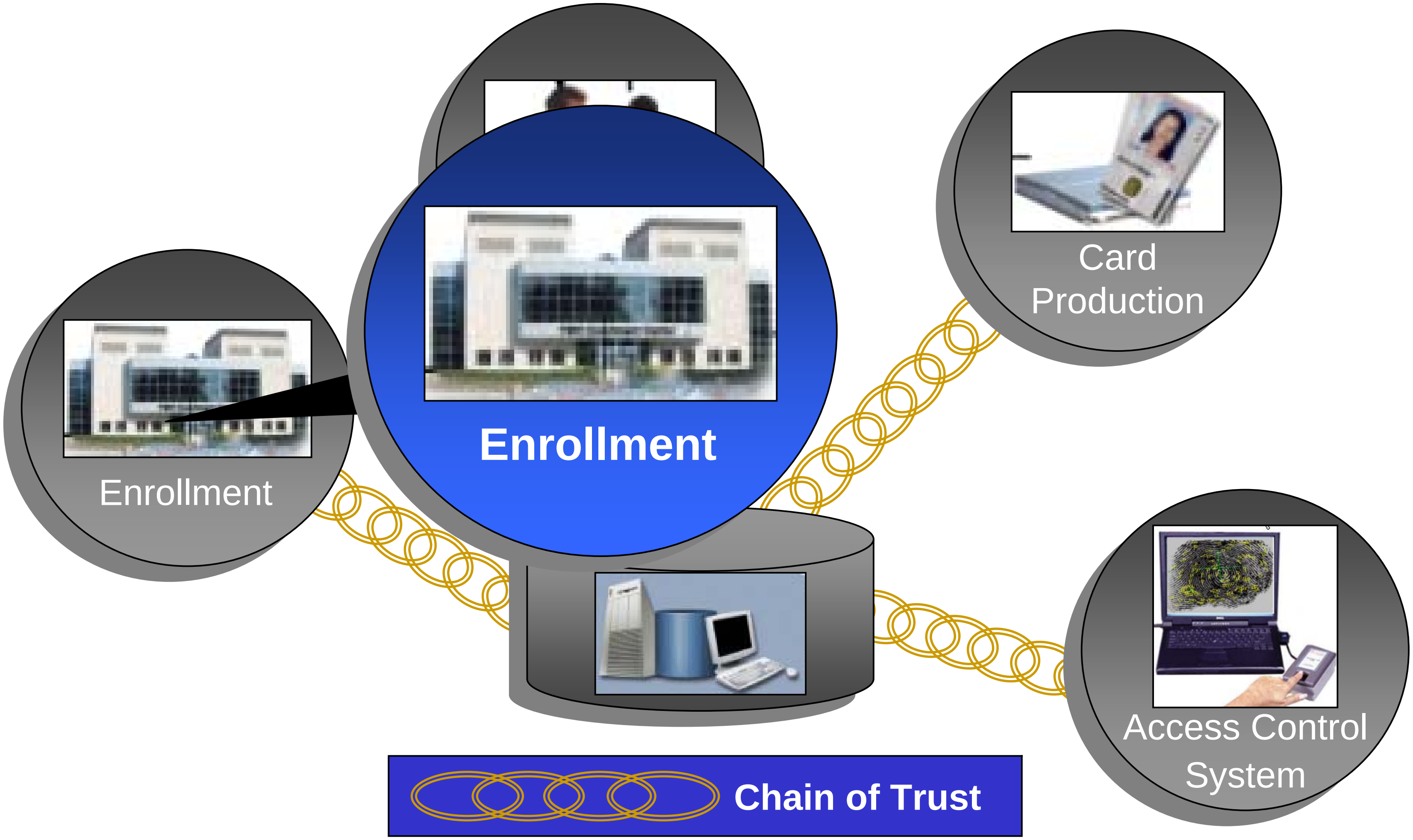
The Identity Management System (IDMS) is made up of the technologies and processes that are employed to validate, capture, store, secure, maintain, and match an individual's identity. IDMS securely manages all aspects of a person's enrollment record information in the TWIC system.

The Chain of Trust requires a secure identity management system that includes the following:

- Secure connectivity between all TWIC system components which include: *enrollment centers** and databases, vetting components, the card production center, and each participating transportation facility;
- Controlled access to personal privacy data;
- Provide a process for system-wide revocation of cardholder privileges; and
- A process for re-issuing the TWIC.

* *Italicized* words are defined in the TWIC Program Definitions section of this brief

Prototype System Components



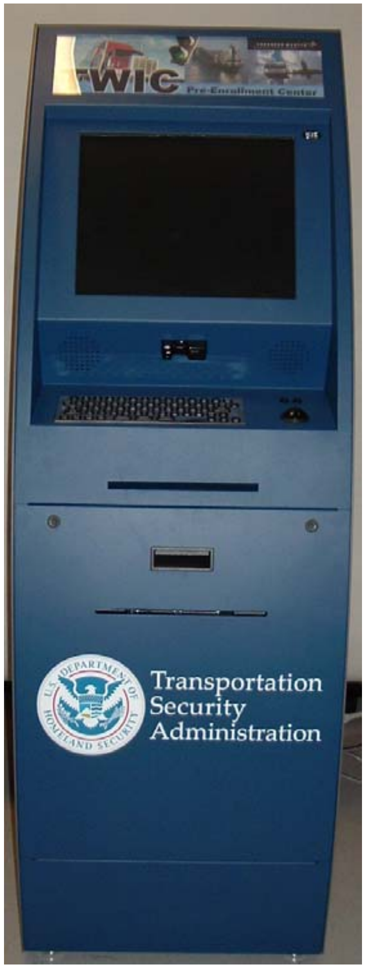
Pre-Enrollment

Objective: To obtain biographical information from the applicant prior to enrollment through the TWIC web site, *enrollment Kiosk*, over the telephone, or in person at the enrollment Center to reduce an individuals enrollment time.

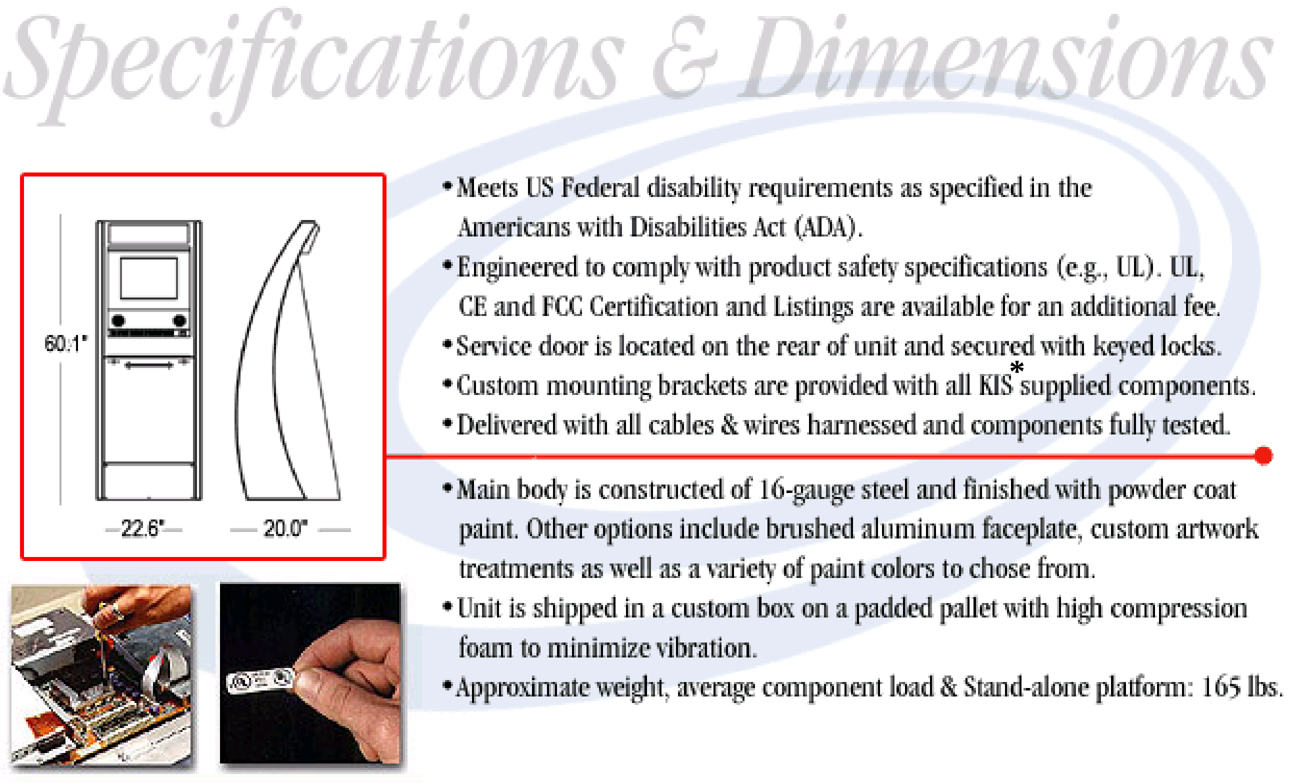
- Pre-enrollment is an optional process;
- The TWIC pre-enrollment process accomplishes the following:
  - Streamlines the enrollment process by providing a means to pre-populate data through the pre-enrollment process;
  - Security of pre-enrollment process; and
  - Improves security by enabling Trusted Agents to spend more time focusing on the claimed identity process rather than data entry during in-person enrollments.
- The TWIC Pre-enrollment process includes the following components:
  - Web site, kiosk, telephone, or in-person;
  - Privacy notice;
  - Assignment of record locator to each applicant;
  - Scheduling capability for in-person enrollment & activation; and
  - Segregation of TWIC portal & TWIC website.

* *Italicized* words are defined in the TWIC Program Definitions section of this brief

TWIC Pre-Enrollment Kiosk



Objective: Pre-enrollment and printing appointment cards as well as other web-based functionality (e.g. card status, lost card reporting, etc.).



Specifications & Dimensions

- Meets US Federal disability requirements as specified in the Americans with Disabilities Act (ADA).
- Engineered to comply with product safety specifications (e.g., UL). UL, CE and FCC Certification and Listings are available for an additional fee.
- Service door is located on the rear of unit and secured with keyed locks.
- Custom mounting brackets are provided with all KIS* supplied components.
- Delivered with all cables & wires harnessed and components fully tested.
- Main body is constructed of 16-gauge steel and finished with powder coat paint. Other options include brushed aluminum faceplate, custom artwork treatments as well as a variety of paint colors to chose from.
- Unit is shipped in a custom box on a padded pallet with high compression foam to minimize vibration.
- Approximate weight, average component load & Stand-alone platform: 165 lbs.

* Kiosk information Systems, Inc.

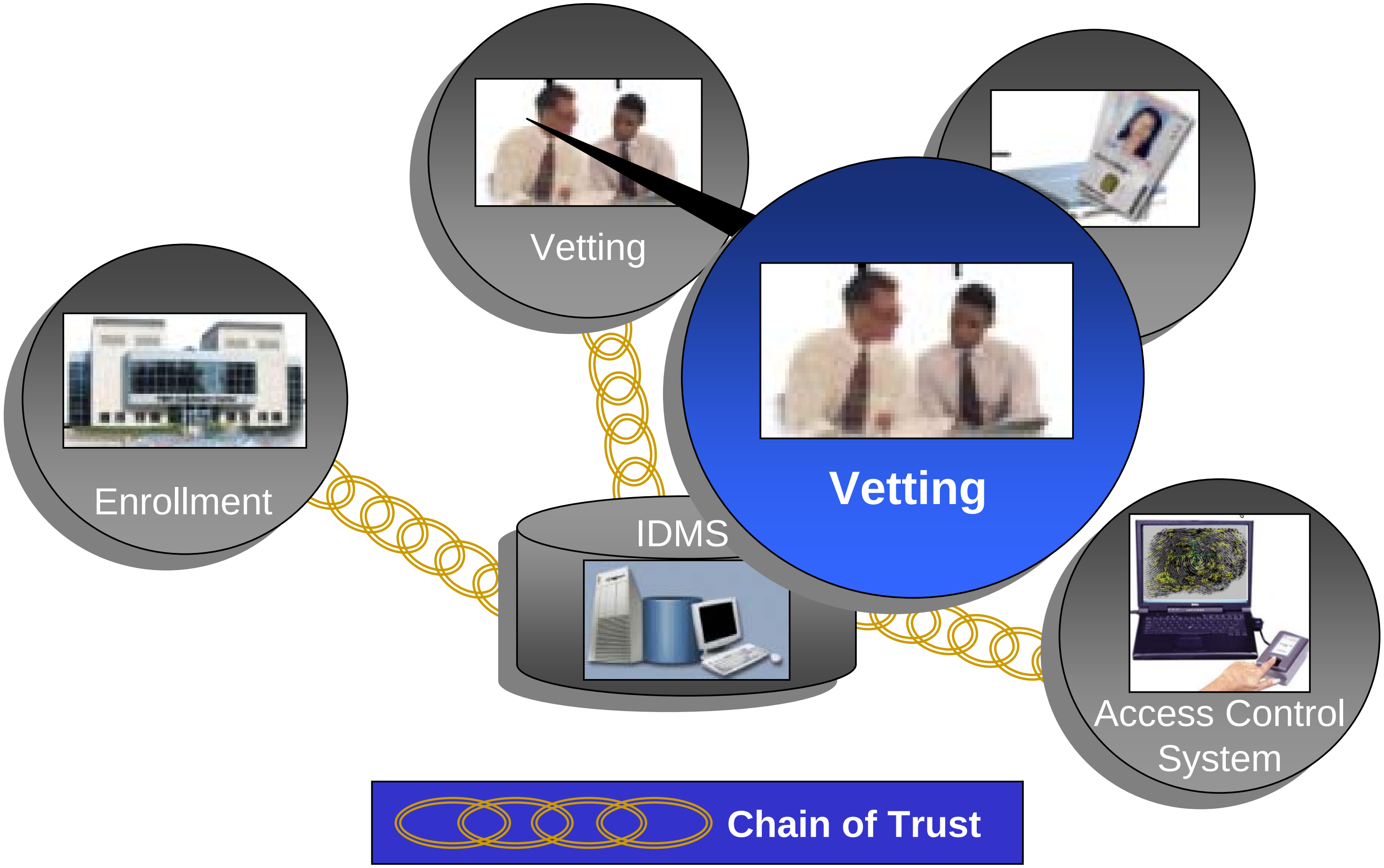
Enrollment

Objective: To produce a complete enrollment record for entry into the IDMS by presenting claimed identity documentation, completing a claimed identity validation, capturing a digital photograph, and providing biometric and biographic information.

- Claimed identity validation requires a face-to-face identity validation and the presentation of *Core identity documents*,* a picture, and biometric data are given to a *Trusted Agent**;
- **The TWIC Enrollment process accomplishes the following:**
  - Protects privacy with secure capture and encryption of enrollment data;
  - Enhances system efficiency by using standard enrollment station configuration and processes;
  - Establishes chain of trust with face to face claimed identity transaction; and
  - Improves security by supporting the detection of fraudulent identity documents through standardized training, automated verification and validation process, document and identity scoring, integrated expert assistance, and standard IT package.
- **The TWIC Enrollment process includes the following components:**
  - Enrollment workstation layout ensures privacy;
  - Pre-enrollment bar code scanning automates pre-enrollment record retrieval (partial or complete);
  - Verification that enrollment data is complete before processing into IDMS; and
  - Reference biometrics are generated from 10-prints captured during enrollment.

* *Italicized* words are defined in the TWIC Program Definitions section of this brief

Prototype System Components



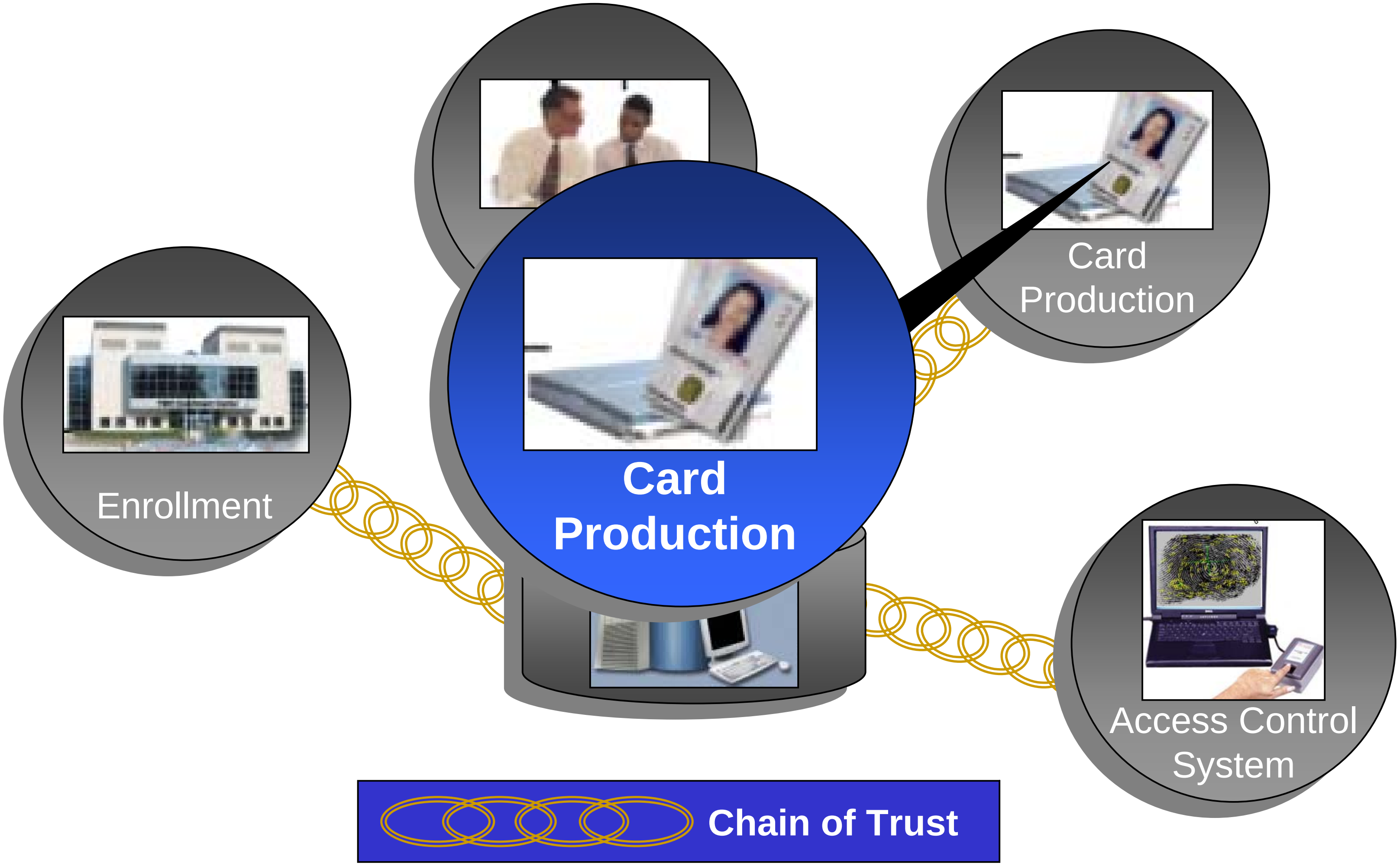
Vetting for the Prototype Phase

Objective: To perform a name-based threat assessment and biometric uniqueness search to determine a transportation worker's eligibility to receive a TWIC.

- **The TWIC Vetting process accomplishes the following:**
  - Performs a threat assessment, using personal information collected to vet against government terrorist related databases to identify individuals who may pose as a risk to transportation security; and
  - Performs a biometric uniqueness (one-to-many) search to limit each person to one biometric identity, resulting in a single TWIC identity.
- **The TWIC Vetting process includes the following components:**
  - Secure connectivity to threat data through Public Key Infrastructure (PKI) encryption. The PKI process includes controlled access to protect personal privacy information; and
  - For TWIC Prototype, the Vetting process for applicants accessing Florida ports also includes a criminal history records check (CHRC)* by the state of Florida. The CHRC is required by Florida law to receive Florida Universal Port Access Credential for access into Florida's 14 deep-water ports.

* The CHRC is required by Florida law to receive a Florida Universal Port Access Credential (FUPAC) for access into Florida's 14 deep water ports.

Prototype System Components



Card Production

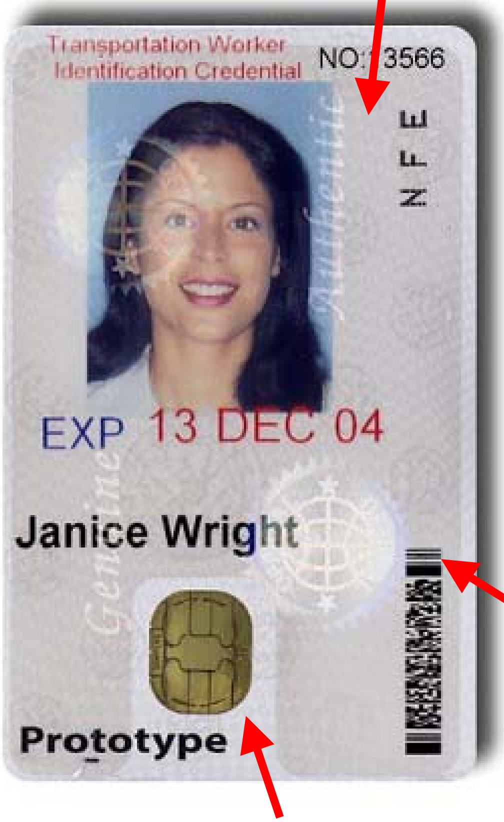
Objective: To manufacture the TWIC, which includes writing, loading, and printing cardholder specific biographic and biometric data to a magnetic stripe, bar code, or integrated circuit chip

- **The TWIC Card Production process accomplishes the following:**
  - Uses advanced technology and security features and high-quality printing;
  - Allows for efficient, economic, and high-capacity output through a centralized process;
  - Standardizes training for production facility operators;
  - Continues the Chain of Trust; secure facility, secure supply chain and inventory management control;
  - Allows for controlled access to protected personal data; and
  - Uses encryption for data transmission, storage, and security.

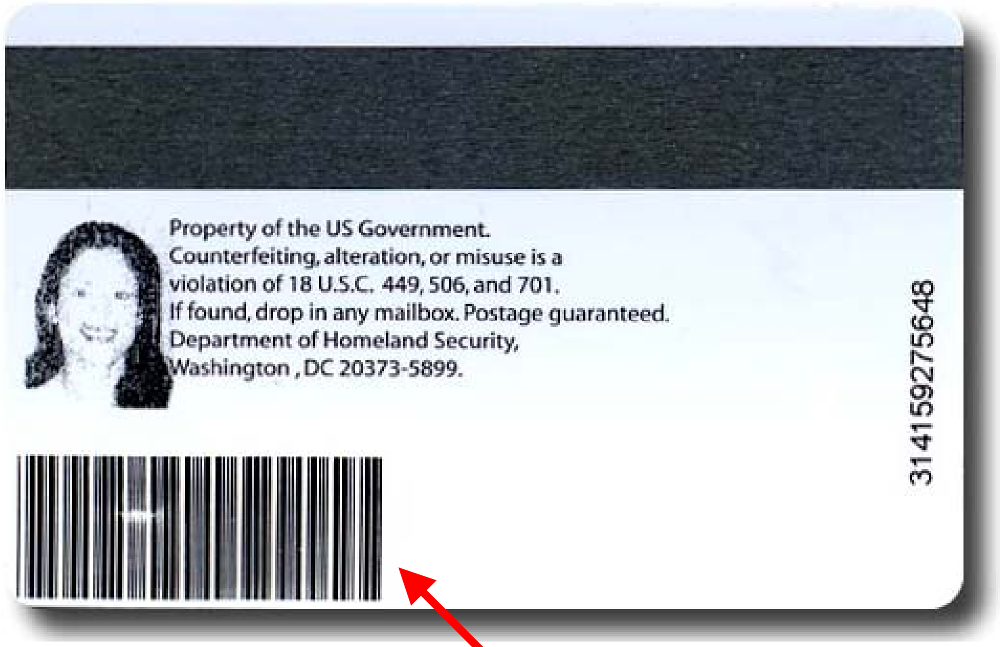
- **The TWIC Card Production process includes the following components:**
  - Conducted only after successful completion of the vetting process;
  - The enrollment record with biometric and biographic information is transmitted through encrypted channels; and
  - Quality assurance checks are performed and the card is electronically locked and sent to the enrollment center.

Prototype Credential

Contactless Chip



Magnetic stripe with FASC-N*
*Federal Agency Smart Credential Number


Property of the US Government.
Counterfeiting, alteration, or misuse is a violation of 18 U.S.C. 449, 506, and 701.
If found, drop in any mailbox. Postage guaranteed.
Department of Homeland Security,
Washington , DC 20373-5899.

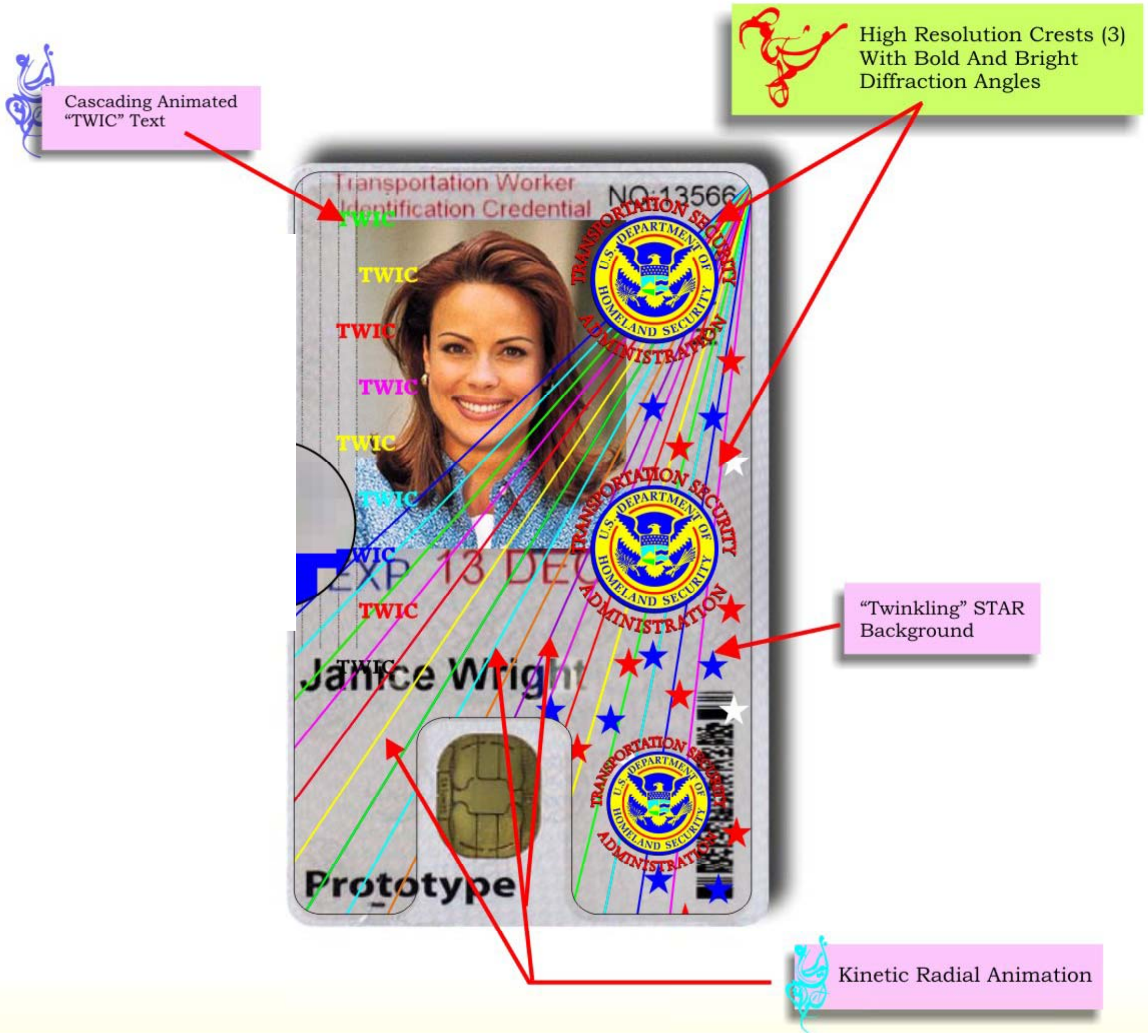
Linear 1D Barcode

Integrated Circuit Chip (ICC)

PDF-417 with Name, GUID*
*Global Unique ID number

Transportation
Security
Administration

Overt Security Features



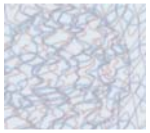
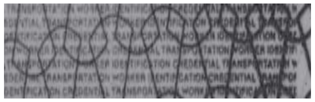
Cascading Animated "TWIC" Text

High Resolution Crests (3) With Bold And Bright Diffraction Angles

"Twinkling" STAR Background

Kinetic Radial Animation

Overt Security Features (continued)

Security Feature	Example	Features / Benefits
Guilloche (1)		Complex printing technique produces an infinite number of curves & patterns resulting in unique, unlimited designs
Guilloche (2)		Gradation of colors achieved by applying line width modulation thereby improving the security feature
Guilloche (3)		Guilloche, although visible, is not easily reproducible; prevents reproduction & counterfeiting
Holographic Overlay		Custom overlays difficult, expensive to replicate; helps prevent copying & counterfeiting; protective layer increases durability
UV Printing		Security feature used in banking. Benefits include low cost & invisibility; prevents reproduction & copying; requires black light
Micro Text (1)		Low cost & not easily reproducible; prevents reproduction & copying; requires magnifying glass or Loupe to detect

Additional Features

Activation (Issuance/Re-Issuance)

Objective: To physically issue the TWIC to the appropriately vetted applicant and "unlock" the card to prepare it for use in the system

- Requires an ID check as well as a reference biometric match to the IDMS in order to activate the TWIC; and
- Takes approximately one minute.

Privilege Granting

Objective: To alert the TWIC IDMS that a local facility has granted a TWIC holder access to their facility

- Worker & card validated in face to face transaction;
- Secure channels protect data exchanges; and
- IDMS registers local privilege granting.

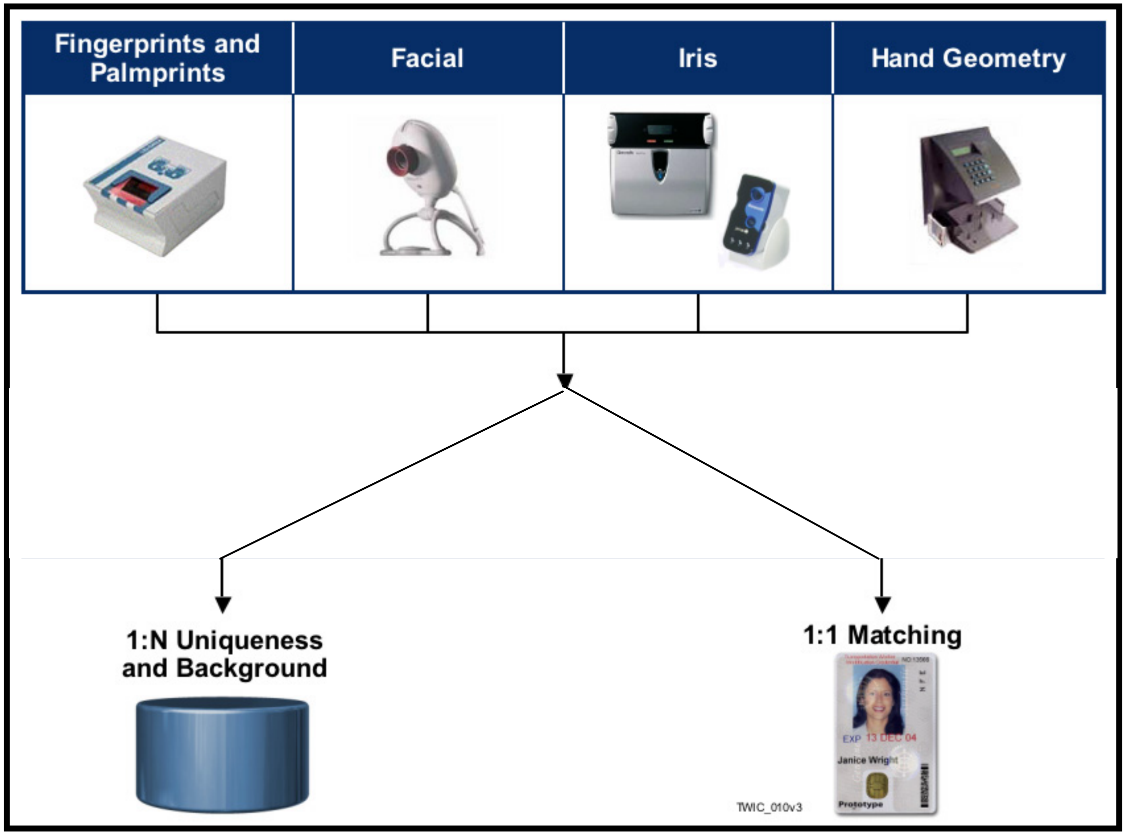
Revocation

Objective: To alert facilities that a TWIC is no longer valid, because it has been lost or stolen or because the TWIC holder is no longer eligible

- Instantaneous card revocation in both physical & logical domains via electronic messaging;
- Supports revocation via standard PKI interfaces (e.g., CRL or OCSP) as well as Hotlist; and
- Revokes based on sites at which access is granted.

Biometrics (Reference & Operational)

- Reference biometrics: right and left index fingers
  - Templates generated from the 10-print image (extracted flats);
  - Ability to add technologies, e.g., iris, hand geometry, facial recognition, etc.; and
  - Alternative process for handling exceptions (e.g., bandaged fingers).
- Operational biometrics:
  - Flexibility to accommodate a broad range of technologies
  - Operational enrollment supports both physical & logical access



TWIC: A Standards-Based Program

The following slides identify many of the standards impacting this Program’s technical and operational specifications.

The TWIC Program views these open standards as the most effective means to achieving reliability and interoperability while promoting a high-level of security and protecting individual privacy.

- TWIC is a standards-based program committed to interoperability and open architecture;
- The TWIC process establishes the chain of trust;
- Derived from years of effort on the part of industry, government, and academia;
- Developed within initiatives sponsored by organizations such as National Institute for Standards and Technology (NIST) and International Committee for Information Technology Standards (INCITS); and
- TWIC was used as a model for the response to HSPD-12, the development of FIPS 201, and SP 800-73.

Standards

Relevant Standard	Where Used
NIST	Total solution must comply with all relevant NIST standards
FIPS 201 (Federal Information Processing Standard)	Federal Credentialing Standard developed in response to HSPD-12. Used in establishing initial unique identity
FIPS 140-1 & 140-2	Cryptographic security for data handling and data storage requirements .
GSC-IS v2.1	All contact & contactless smart cards, middleware, and readers
GSC-IAB TIG SCEPACS v2.2	Defines the Card Holder Unique ID numbering schema. (Interagency Advisory Board Technical Implementation Guidance for Smart Card Enabled Physical Access Control Systems)
ISO 7810	All identification cards physical characteristics
ISO 7816, 1-10	All contact cards (JavaCard)
ISO 14443-A	All contactless cards (DESFire & OCS) & readers
ISO 15693	Not used; vicinity cards not planned
SEIWG 012 **(Now FASC-N)**	Mandatory field incorporated into the Card Holder Unique ID number described in GSC-IAB TIC SCEPACS v2.2.
Global Platform	All contact cards (JavaCard) for post-issuance updating
X.509 v3	Used at all cryptographic authentication points and for certificates on card

Standards (continued)

Relevant Standard	Where Used
ICAO 9303	The international standard influenced various useful elements specific to MRTD performance .(Machine Readable Travel Documents)
CBEFF NISTIR 6529	Standardizes all data elements and data structure for packaging biometric information
ANSI/NIST-ITL 1-2000	Quality & formatting of 10-print & 1:N fingerprint images
ANSI/X9 X9.84-2003	Biometric information mgmt & security; applicable requirements related to biometric data protection
INCITS 383	Biometric application profile for identity verification of transportation workers - applicability & tailoring of relevant biometric standards
INCITS 358 (BioAPI)	Biometric technology provider generic high-level authentication model for enrollment, verification, identification and data management.
ANSI/INCITS 377	Standard biometric finger pattern template for verification Stored on the ICC
ANSI/INCITS 378	Standard biometric finger minutiae template for verification. Stored on the ICC
SP 800-73	TBD
SP 800-76	TBD

Homeland Security Presidential Directives

- Presidential directives are a form of executive order issued by the President of the United States with the advice and consent of the National Security Council.
- On October 29, 2001, George W. Bush designated special presidential directives called Homeland Security Presidential Directives, or HSPDs, to be issued by the President of the United States with the advice and consent of the Homeland Security Council.
- As of January 2005, there have been 12 HSPDs, the last two of which address issues specifically relating to the TWIC Program.

Homeland Security Presidential Directives 11 and 12

HSPD 11*

Homeland Security Presidential Directive 11 (HSPD-11) is a policy for comprehensive terrorist-related screening procedures.

HSPD 12**

Homeland Security Presidential Directive 12 (HSPD-12) is a policy for a common identification standard for federal employees and contractors – (Secure and Reliable Forms of Identification).

The TWIC Program was used as a model for the development of federal policy on identity management and credentialing, as stated in FIPS 201, SP 800-73 and SP 800-76.

- Issued based on sound criteria for verifying an individual employee's identity;
- Strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
- Can be rapidly authenticated electronically; and
- Issued only by providers whose reliability has been established by an official accreditation process.

* For more information visit: www.whitehouse.gov/news/releases/2004/08/20040827-7.html

** For more information visit: www.whitehouse.gov/news/releases/2004/08/20040827-8.html

TWIC Program Definitions/Acronyms

- **ANSI –** American National Standards Institute
- **Biometrics –** Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic that are unique to an individual. Physical biometrics include fingerprints, hand geometry, facial patterns, and iris and retinal scans. Behavioral biometrics include voice patterns, written signatures, and keyboard typing techniques.
- **Card Management System (CMS) –** Manual and automated processes that are used to procure, control, track, sustain, and manage card issuance and support a card throughout it's life cycle; required to register, re-issue, deactivate, and/or revoke cardholders' cards, and interface with source data systems to support issuance of watch or threat lists of writing, loading, and/or printing cardholder specific biographic (i.e. name) and/or biometric (facial .
- **CBEFF –** Common Biometric Exchange File Format
- **Claimed Identity –** The person (name and background) an individual alleges to be prior to validation and verification.
- **Contactless Smart Card –** A smart card that can exchange information with a card reader without coming in physical contact with the reader, using 13.56-megahertz radio frequency transmissions to exchange information with card readers; the contactless chip is typically used for applications demanding fast transaction times.

TWIC Program Definitions (continued)

- **Core identity documents –** Government-issued documents that provide the basis for issuing all other identity documents, usually a birth certificate and a national identity number. Governments regard the issuance core identities as a crucial function closely tied to both security and access to benefits.
- **Database –** A collection of logically related data stored together in one or more computerized files.
- **Enrollment Center –** Physical location (facility) where card enrollment functions are performed.
- **Enrollment Station (Kiosk) –** A computer workstation used for enrollment.
- **Facility –** A location whose function enables commerce as part of the national transportation system. These transportation systems include maritime, aviation, transit, rail, and other surface transportation modes (e.g. port terminals and administrative buildings).
- **FIPS** Federal Information Processing Standards
- **GSC-IS –** Government Smart Card-Interoperability Specification
- **ICAO –** International Civil Aviation Organization
- **Identity Management (IDM) –** The process of validating, capturing, storing, securing, maintaining, and matching an individual’s identity.

TWIC Program Definitions (continued)

- **INCITS –** International Committee for Information Technology Standards
- **Integrated Circuit Chip (ICC) –** A small piece of thin semiconductor material, such as silicon, that has been chemically processed to have a specific set of electrical characteristics such as circuits, storage, or logic elements.
- **ISO –** International Organization for Standardization
- **NIST –** National Institute of Standards and Technology
- **NISTIR –** National Institute of Standards and Technology Interagency Reports
- **SEIWG –** Security Equipment Integration Working Group
- **Public Key Infrastructure (PKI) Encryption –** A system of hardware, software, policies, and people that provide a suite of information security assurances, including confidentiality, data integrity, authentication, and non-repudiation that are implemented to protect sensitive communications and transactions.
- **Revocation –** The process of ending the validity of a digital identity, credential, or token.
- **Transportation Mode –** Types of transportation-related entities, including maritime, aviation, mass transit, rail, and pipeline.

TWIC Program Definitions (continued)

- **Transportation Worker –** Any owner, operator, employee, or contractor assisting or engaged in supporting the national transportation system; e.g. individuals involved in the movement of cargo, sale of goods within a transportation facility, or the development and maintenance of information technology systems. Any person within the transportation industry whose job requires unescorted access to a secure area of transportation industry site.
- **Trusted Agent –** A person or group of people granted authority by the Federal Government to conduct card enrollment.

For additional information…

E-mail the TWIC Program at

Credentialing@dhs.gov

U.S. DEPARTMENT OF HOMELAND SECURITY

Transportation
Security
Administration